Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
27 OCT 2014	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Security Engineering Risk Analysis (SERA)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Woody /Carol	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

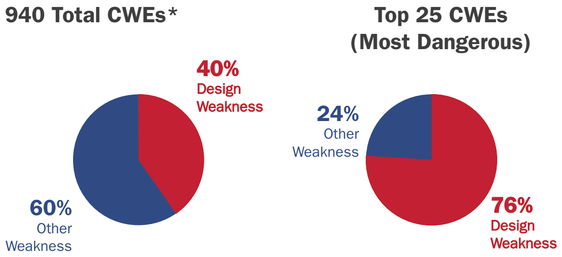
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**1**	

Security Engineering Risk Analysis (SERA)

"We wouldn't have to spend so much time, money, and effort on network security if we didn't have such bad software security."

Bruce Schneier in Viega and McGraw, *Building Secure Software*, 2001

Importance of Good Design

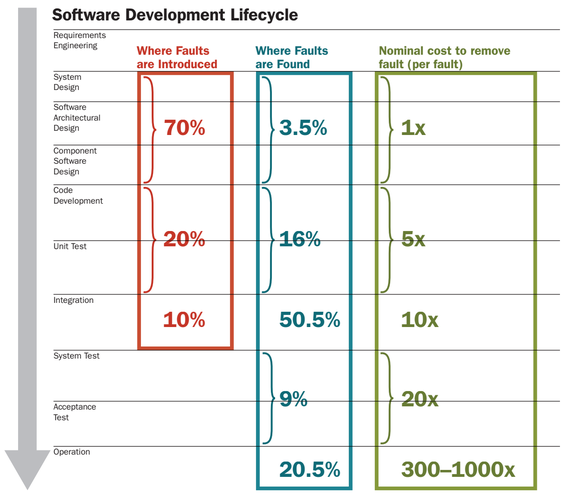


***MITRE's Common Weakness Enumeration (CWE)**
Source: http://cwe.mitre.org/ as of Feb 9, 2014

Software Faults: Introduction, Discovery, and Cost

Faults account for 30–50% percent of total software project costs.

- Most faults are introduced before coding (~70%).
- Most faults are discovered at system integration or later (~80%).



Errors during requirements engineering are costly!

- Defects cost up to 200 times more once fielded than if caught in requirements engineering
- Reworking defects consumes >50% of project effort
- >50% of defects are introduced in requirements engineering

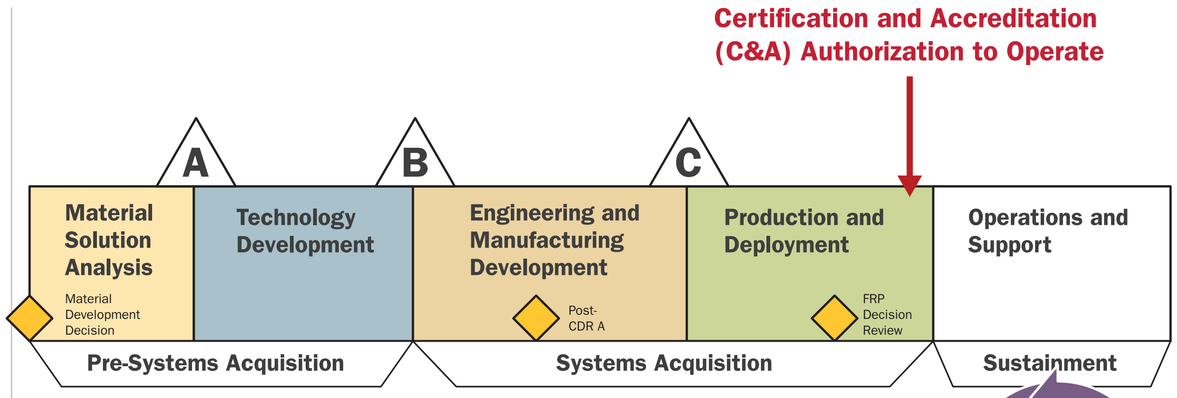
Goal: Reduce Security Design Risk

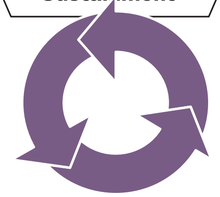
Security design weaknesses

- Are not addressed by security controls or static analysis tools and
- Cannot be easily addressed during operations (e.g., by patching systems)

Applying SERA during requirements specification

- Provides early detection of design weaknesses for remediation
- Reduces residual security risk during operations





Security Engineering Risk Analysis

1. Establish operational context.

2. Identify risk.

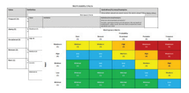
3. Analyze risk.

4. Develop control plan.

Modeling Techniques

Risk Identification Worksheet

Risk Evaluation Criteria



Risk Analysis Worksheet

Control Approach Worksheet

Control Plan Worksheet

Software Engineering Institute | Carnegie Mellon University

Contact: Carol Woody cwoody@cert.org